実二次体上の不定方程式 $X^3 = u + 27v$, $X^3 = u + v$ について

加川 貴章 (立命館大学)

1 Introduction

k を実二次体, $\mathcal{O}_k$ を整数環, $\mathcal{O}_k^\times$ を単数群とする. $X \in \mathcal{O}_k - \{0\}$, $u, v \in \mathcal{O}_k^\times$ を解とする実二次体上の不定方程式

$$X^3 = u + 27v, \tag{1}$$
$$X^3 = u + v \tag{2}$$

を考える. $\mathcal{O}_k^\times$ は無限集合であるから, (1), (2) の解を求めることは非自明な問題である. そうは言っても, (1), (2) を考えるのは凄くマニアックに見えるだろう. しかしこれらは楕円曲線に関するある研究から出てきたもので, 不自然なものではない (2 節で説明する). 最近の筆者の興味は楕円曲線から離れて, 方程式そのものにあるが. この稿では, (1), (2) に関して得られている結果を報告する.

2 EGR を持つ楕円曲線

元々考えていたのは次の問である:

問. k を代数体, S を k の素イデアルの有限集合とする. k 上定義された S の外 good reduction を持つ楕円曲線 (の k 上の同型類) を決定せよ. (Shafarevich により同型類は有限個であることが示されている.)

$S = \emptyset$ の時, S の外 good reduction を持つことを「至る所 good reduction (everywhere good reduction, EGR と略す) を持つ」という.

定理 2.1 (Tate)**.** $\mathbb{Q}$ 上 EGR を持つ楕円曲線は存在しない.[1]

証明. $\mathbb{Q}$ 上 EGR を持つ楕円曲線 E が存在するとする. $\mathbb{Q}$ の類数は 1 なので, [20], Chapter VIII の Corollary 8.3 より, E は $\mathbb{Z}$ 係数の Weierstrass 方程式で判別式 Δ が ± 1 であるもので定義される:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}, \quad \Delta = \pm 1.$$

$b_2, b_4, b_6, b_8, c_4, c_6$ を通常通りに

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

[1] Tate は証明を公表していない. Ogg は [16] で証明を与えているがその証明は一箇所変だと思しき場所がある. 以下の証明は [20] の演習問題に付いているヒントを考慮に入れて, [16] の証明を修正したものである.

と定義する. $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = (c_4^3 - c_6^2)/1728$ である.

a_1 が偶数であるとすると, $4 \mid b_2, 2 \mid b_4$ である. よって $\pm 1 = \Delta \equiv -27b_6^2 \equiv 5b_6^2 \pmod 8$ が得られ, $b_6^2 \equiv \pm 3 \pmod 8$ となり不合理. 従って a_1 は奇数でなければならないので, $b_2 \equiv a_1^2 \equiv 1 \pmod 4$, $c_4 \equiv b_2^2 \equiv 1 \pmod 8$ である. $c_4 = x \pm 12$ ($x \in \mathbb{Z}$, 複号は Δ と同順) とすると, $c_6^2 = c_4^3 \mp 1728 = x(x^2 \pm 36x + 432)$ である.

$$x = c_4 \mp 12 \equiv c_4 + 4 \equiv 5 \pmod 8 \tag{3}$$

が成り立つ. $x(x^2 \pm 36x + 432) = c_6^2 \geq 0$, $x^2 \pm 36x + 432 = (x \pm 18)^2 + 108 > 0$ で, $x \equiv 5 \pmod 8$ より $x \neq 0$ だから, $x > 0$ である. p ($\neq 3$) を x の素因数とする. $x \equiv 5 \pmod 8$ より $p \neq 2$ である. $x^2 \pm 36x \equiv 0 \pmod p$, $432 \not\equiv 0 \pmod p$ より, $\mathrm{ord}_p(x(x^2 \pm 36x + 432)) = \mathrm{ord}_p(x)$ である. 一方 $\mathrm{ord}_p(x(x^2 \pm 36x + 432)) = \mathrm{ord}_p(c_6^2) = 2\,\mathrm{ord}_p(c_6)$ は偶数である. 故に $x = \square_{\mathbb{Q}}$ または $x = 3\square_{\mathbb{Q}}$ である.[2] これより $x \equiv 1 \pmod 8$ または $x \equiv 3 \pmod 8$ が従うが, これは (3) に反する. □

別証明. $\mathbb{Q}$ 上 EGR を持つ楕円曲線 E が存在するとする. $\mathbb{Z}$ 係数の Weierstrass 方程式で判別式が ± 1 であるものをとる. c_4, c_6 を上の通り定義すると, $c_4^3 - c_6^2 = \pm 1728$ が成り立つ. $E_\pm$ を $y^2 = x^3 \pm 1728$ で定義される楕円曲線とすると, $E_\pm(\mathbb{Q}) = \langle (\mp 12, 0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$ である. ([21] の Chapter 2, 3 に出ている方法で求められる. 但し, $E_\pm$ の global minmal model である $y^2 = x^3 \pm 27$ で考えた方がよい. もしくは [1] により $y^2 = x^2 \pm 27$ はどちらも階数 0 で, torsion 群の位数は 2 であることが分かる. $y^2 = x^3 + 27$ は 144A3, $y^2 = x^3 - 27$ は 36A3 というラベルが振られている.) よって E の c_4, c_6 の候補 C_4, C_6 は $C_4 = \pm 12$, $C_6 = 0$ のみなので, E は

$$E_1 : y^2 = x^3 - \frac{1}{4}x, \quad E_2 : y^2 = x^3 + \frac{1}{4}x$$

のいずれかと $\mathbb{Q}$ 上同型. ($y^2 = x^3 - (C_4/48)x - (C_6/864)$ の c_4 は C_4, c_6 は C_6 である.) E_1 の global minimal な定義方程式は $y^2 = x^3 - 4x$ で, これの判別式は 2^{12}, 導手は 64, E_2 の global minimal な定義方程式は $y^2 = x^3 + 4x$ で, これの判別式は -2^{12}, 導手は 32 である. (いずれも Tate のアルゴリズムで求まる.) よって E は 2 で bad reduction を持ち矛盾. □

Tate のアルゴリズムの代わりに, 次の Kraus の定理 ([14]) を使ってもよい.

定理 2.2. $C_4, C_6 \in \mathbb{Z}$ が $(C_4^3 - C_6^2)/1728 \in \mathbb{Z} - \{0\}$ を満たすとする. この時 $\mathbb{Q}$ 上定義された楕円曲線の $\mathbb{Z}$ 係数の定義方程式でその方程式の c_4, c_6 が C_4, C_6 であるものが存在することと以下の (1), (2) が成り立つことは同値である.

(1) $C_6 \not\equiv \pm 9 \pmod{27}$.

(2) $C_6 \equiv -1 \pmod 4$ または [$C_4 \equiv 0 \pmod{16}$ かつ $C_6 \equiv 0, 8 \pmod{32}$].

$C_4 = \pm 12, C_6 = 0$ は定理 2.2 の条件を満たさないので, $c_4 = \pm 12$, $c_6 = 0$ である $\mathbb{Z}$ 係数の Weierstrass 方程式は無い.

次に二次体の場合を考えたい. k が虚二次体で $(h_k, 6) = 1$ (以降代数体 k の類数を h_k と書く) の時, k 上 EGR を持つ楕円曲線は無い ([3], [18], [22]). $(h_k, 6) \neq 1$ の場合だとどうかというと, $\mathbb{Q}(\sqrt{-65})$ (類数 8) の上に EGR を持つ楕円曲線が 8 本あると Setzer が [18] において主張している. (横山俊一氏の指摘通り, [18] には曲線の定義方程式は出ていない. 横山氏の研究室所属の生川青輝氏がこれらの定義方程式を明示的に構成したとのアナウンスが本集会であった.)

次は実二次体の場合だが, この場合は類数 1 の体上にも例がある.

[2] 以下代数体 k の平方元を $\square_k$ と書くことにする.

例 2.3 (Tate)**.** $\varepsilon_{29} = (5+\sqrt{29})/2$ を $\mathbb{Q}(\sqrt{29})$ (類数は 1) の基本単数とする. 楕円曲線

$$y^2 + xy + \varepsilon_{29}^2 y = x^3$$

は $\mathbb{Q}(\sqrt{29})$ 上 EGR を持つ. 実際この曲線の判別式は $-\varepsilon_{29}^{10}$ である.

実二次体上には興味深い楕円曲線がある. k を実二次体, N を k の判別式とする. 保型形式の空間 $S_2(\Gamma_0(N), \left(\frac{*}{N}\right))$ が 2 次元の因子を持てば, $\mathbb{Q}$-simple な 2 次元アーベル多様体 A_N が作られる. k 上で A_N は $A_N = B_N \times B'_N$ と分解され, B_N, B'_N は k 上定義された EGR を持つ楕円曲線である. B_N を志村の楕円曲線という. [15] で次の定理が証明されている.

定理 2.4. 例 2.3 の楕円曲線は B_{29} と $\mathbb{Q}(\sqrt{29})$ 上 isogenous である.

実二次体上 EGR を持つ楕円曲線と志村の楕円曲線の関係を調べることは興味深い (ある種の modularity 問題である). 正直筆者は [15] の証明をちゃんと理解したとは言えない. 難しかった. そこで思ったのは, この手の定理の一番「安直」な証明方法は, EGR を持つ楕円曲線を全て決定してしまうことであろう, と. ということで実二次体 k が与えられ時, k 上 EGR を持つ楕円曲線を決定するわけである.[3]

k を実二次体とし, E を判別式が k の単数である $\mathcal{O}_k$ 係数の Weierstrass 方程式で定義される楕円曲線とする. ([18] において, $(h_k, 6) = 1$ ならば k 上 EGR を持つ楕円曲線は全てこのような方程式で定義されることが証明されている. 任意の代数体上で構わない.) 決定の方針は定理 2.1 の別証明と同様である. 即ち ε (> 1) を k の基本単数とし, c_4, c_6 を通常の通りに定義すると, $c_6^2 = c_4^3 \pm 1728\varepsilon^n$ である $n \in \mathbb{Z}$ が存在する. $-6 \leq n < 6$ としてよい. よって

$$y^2 = x^3 \pm 1728\varepsilon^n \ (-6 \leq n < 6)$$

を満たす $x, y \in \mathcal{O}_k$ を決定すればよい. しかし n が沢山あり, 複号もあるので, 全てを決定するのは大変である. そこで色々工夫し, 2 等分点の体を用いた議論 ([5] 参照) で符号や n の偶奇に制限が付けられたり, 3 等分点の体を用いた議論 ([4] 参照) により, n の 3 での可除性が分かったりして, 手間を減らせる. 3 等分点の体を用いた議論の過程で 3 次の isogeny を調べる必要が出てきた. それについて以下説明する. 代数体 k と k の整因子 $\mathfrak{m}$ (整イデアルと無限素点の形式的な積) に対し, $\mathfrak{m}$ を法とする ray class number を $h_k(\mathfrak{m})$ と書く.

定理 2.5. k を実二次体とする. $4 \nmid h_k((3)\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)})$ ($\mathfrak{p}_\infty^{(1)}, \mathfrak{p}_\infty^{(2)}$ は k の実無限素点) もしくは $4 \nmid h_{k(\sqrt{-3})}((\sqrt{-3}))$ が成り立つとする. この時 k 上 EGR を持つ楕円曲線で判別式が 3 乗数であるもの (もしあれば) から他の楕円曲線への k 上定義された 3 次の isogeny がある.

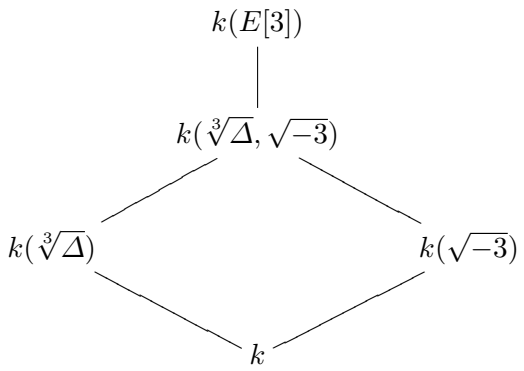
定理 2.6. k を $(h_k, 6) = 1$ なる実二次体, ε (> 1) を k の基本単数, $\mathfrak{P}_\infty^{(1)}, \mathfrak{P}_\infty^{(2)}$ を $k(\sqrt[3]{\varepsilon})$ の実無限素点とする. $4 \nmid h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)})$ もしくは $4 \nmid h_{k(\sqrt[3]{\varepsilon}, \sqrt{-3})}((\sqrt{-3}))$ とする. この時 k 上 EGR を持つ楕円曲線で判別式が 3 乗数でないもの (もしあれば) から他の楕円曲線への k 上定義された 3 次の isogeny がある.

定理 2.5, 定理 2.6 の証明の概略は以下の通り (詳細は [7] を参照せよ):

E を k 上定義された楕円曲線とすると, Néron–Ogg–Shafarevich の criterion により $k(E[3])/k$ で分岐しうる素点は, E の bad prime, 3 の素因子, 及び無限素点だけである. (ここで $E[3] =$

[3] 安直でないことは段々分かってきたが.

$\{P \in E \mid 3P = O\}$ (O は無限遠点) で, $k(E[3])$ は k に $E[3]$ の O 以外の全ての点の x 座標, y 座標を添加した体である.) $k(E[3])$ は $\sqrt[3]{\Delta}, \sqrt{-3}$ を含んでいる (Δ は E の判別式).



$\mathrm{Gal}(k(E[3])/k)$ は $\mathrm{GL}_2(\mathbb{F}_3)$ (位数 48 の非可換群) の部分群と同型である. [7] で $\mathrm{GL}_2(\mathbb{F}_3)$ の部分群を分類している. こういったことを使うと, E が k 上 EGR を持つとすると, k, $k(\sqrt{-3})$, $k(\sqrt[3]{\Delta})$, $k(\sqrt[3]{\Delta}, \sqrt{-3})$ 上に 3 と無限素点の外不分岐なアーベル拡大を作れる. (Δ が k の 3 乗数ならば, $k(\sqrt[3]{\Delta}) = k$, $k(\sqrt[3]{\Delta}, \sqrt{-3}) = k(\sqrt{-3})$ であることに注意.) Ray class number の非可除性を仮定しておけば, $\mathrm{Gal}(k(E[3])/k)$ の形が限定され, 主張が従うのである.

E_1, E_2 を代数体 k 上定義された楕円曲線とする. E_1 から E_2 への k 上定義された 3 次の isogeny が存在するとする. この時 $j(E_1)$, $j(E_2)$ をそれぞれ E_1, E_2 の j 不変量とすると, $j(E_1) = J(t_1)$, $j(E_2) = J(t_2)$, $t_1 t_2 = 3^6 = 729$ である $t_1, t_2 \in k$ が存在する. ここで

$$J(X) = \frac{(X + 27)(X + 3)^3}{X}.$$

よって $c_4(E_1), c_6(E_1), \Delta(E_1)$ を通常通りに定義すると,

$$j(E_1) = \frac{c_4(E_1)^3}{\Delta(E_1)} = \frac{(t_1 + 27)(t_1 + 3)^3}{t_1},$$
$$j(E_1) - 1728 = \frac{c_6(E_1)^2}{\Delta(E_1)} = \frac{(t_1^2 + 18t_1 - 27)^2}{t_1}$$

が成り立つ. k が実二次体で $E = E_1$ が k 上 EGR を持つとすると,

- $j(E) \in \mathcal{O}_k$ (cf. [20], Chapter VII, Proposition 5.5);
- 単項イデアル ($\Delta(E)$) はある整イデアルの 12 乗;
- $j(E) \neq 0, 1728$ ([19])

が成り立つ. よって $j(E) = J(t)$ であるとき, (t) がある整イデアルの 6 乗であることが証明出来る (割と簡単な議論で済む. 詳細は [7] を参照せよ). よって

$$(t) = \begin{cases} (1), (3^6) & (3 \text{ が } k \text{ で惰性する時}) \\ (1), (3^3), (3^6) & (3 \text{ が } k \text{ で分岐している時}) \\ (1), \mathfrak{p}^6, \mathfrak{p}'^6, (3^6) & ((3) = \mathfrak{p}\mathfrak{p}', \mathfrak{p} \neq \mathfrak{p}' \text{ の時}) \end{cases}$$

となる. 3 つ目の場合は, $\mathfrak{p}, \mathfrak{p}'$ が単項イデアルでないかもしれないし, 単項イデアルであったとしても生成元は体に依存した数になり, 統一的な取り扱いは難しいと思われる. よってこの場

合は除いて, $(t)=(1),(3^3),(3^6)$ の時を考える. $(t)=(1)$ ならば

$$\left(\frac{c_4(E)}{t+3}\right)^3 = \Delta(E)(1+27w),\quad w=\frac{1}{t}\in\mathcal{O}_k^\times, \tag{4}$$

$(t)=(3^6)$ ならば

$$\left(\frac{3c_4(E)}{t+3}\right)^3 = \Delta(E)(w+27),\quad w=\frac{3^6}{t}\in\mathcal{O}_k^\times, \tag{5}$$

$(t)=(3^3)$ ならば

$$\left(\frac{c_4(E)}{t+3}\right)^3 = \Delta(E)(1+w),\quad w=\frac{3^3}{t}\in\mathcal{O}_k^\times. \tag{6}$$

よって E が global minimal な方程式で定義されていれば, $\Delta(E)\in\mathcal{O}_k^\times$ なので, (1), (2) が出てくるのである. ($j(E)\neq 0$ より $c_4(E)\neq 0$ なので, $X\neq 0$ である.)

3 $X^3=u+27v$

まず (1) に関する結果を挙げる.

定理 3.1 ([6])**.** k を実二次体とする. (1) が u が 3 乗数である解を持つのは $k=\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{33})$ の時のみで, $k=\mathbb{Q}(\sqrt{6})$ の時の解は

$$(X,u,v)=((4+\sqrt{6})\varepsilon_6^n,\varepsilon_6^{3n},\varepsilon_6^{3n+1}),((4-\sqrt{6})\varepsilon_6^n,\varepsilon_6^{3n},\varepsilon_6^{3n-1}),$$

$k=\mathbb{Q}(\sqrt{33})$ の時の解は

$$(X,u,v)=((-5-\sqrt{33})\varepsilon_{33}^n,\varepsilon_{33}^{3n},-\varepsilon_{33}^{3n+1}),((-5+\sqrt{33})\varepsilon_{33}^n,\varepsilon_{33}^{3n},-\varepsilon_{33}^{3n-1}).$$

ここで $n\in\mathbb{Z}$ は任意で, $\varepsilon_6=5+2\sqrt{6}$, $\varepsilon_{33}=23+4\sqrt{33}$ はそれぞれ $\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{33})$ の基本単数である.

証明. 解があるとする. 必要なら (1) の両辺に 3 乗数を掛けて, $u=1$ としてよい. $27v=X^3-1=(X-1)(X^2+X+1)$ としてノルムをとると,

$$\begin{aligned}3^6N_{k/\mathbb{Q}}(v)&=x^3-y^3+3xy+1\\&=(x-y+1)(x^2+y^2+1+xy+y-x).\end{aligned}\tag{7}$$

ここで $x:=N_{k/\mathbb{Q}}(X), y:=\mathrm{Tr}_{k/\mathbb{Q}}(X)$. $3^6N_{k/\mathbb{Q}}(v)$ は奇数だから, (7) より $x+y+xy+1\equiv 1 \pmod 2$. よって $(x+1)(y+1)\equiv 1 \pmod 2$ なので $x\equiv y\equiv 0 \pmod 2$ である. 従って再び (7) より $N_{k/\mathbb{Q}}(v)\equiv 3^6N_{k/\mathbb{Q}}(v)\equiv 1 \pmod 4$ なので, $N_{k/\mathbb{Q}}(v)=1$ である.

$$x^2+y^2+1+xy+y-x=\frac{(x+y)^2+(y+1)^2+(x-1)^2}{2}\geq 0$$

なので, $0\leq a\leq 6$ なる $a\in\mathbb{Z}$ に対し,

$$x-y+1=3^a,\quad x^2+y^2+1+xy+y-x=3^{6-a}.$$

x を消去すると,

$$3y^2+(3^{a+1}-3)y+(3^{2a}+3-3^{a+1}-3^{6-a})=0.$$

$a=0,6$ の時は左辺が 3 で割り切れないので不可能なので, $1\le a\le 5$ である. 左辺を 3 で割った 2 次式の判別式は

$$-3^{2a-1}+2\times 3^a-3+4\times 3^{5-a}$$

で, これが $\square_{\mathbb{Q}}$ となるのは $a=1$ の時のみであり, その時根は $y=8,\ -10$ である. よって $(\mathrm{Tr}_{k/\mathbb{Q}}(X),N_{k/\mathbb{Q}}(X))=(8,10)$ (即ち $X=4\pm\sqrt{6}$), または $(\mathrm{Tr}_{k/\mathbb{Q}}(X),N_{k/\mathbb{Q}}(X))=(-10,-8)$ (即ち $X=-5\pm\sqrt{33}$) である. □

定理 3.2 ([7])**.** k を実二次体とする. (1) が $uv=\pm\square_k$ なる解を持つのは $k=\mathbb{Q}(\sqrt{29})$ の時のみで, 解は $(X,u,v)=(\pm\varepsilon_{29}^{n},\mp\varepsilon_{29}^{3n-4},\pm\varepsilon_{29}^{3n-2})$, $(\pm\varepsilon_{29}^{n},\mp\varepsilon_{29}^{3n+4},\pm\varepsilon_{29}^{3n+2})$. ここで $n\in\mathbb{Z}$ は任意で, $\varepsilon_{29}=(5+\sqrt{29})/2$ は $\mathbb{Q}(\sqrt{29})$ の基本単数である.

証明. 解があるとする. 必要なら u^3 を (1) の両辺に掛けて, $N_{k/\mathbb{Q}}(u)=1$ としてよい. すると $uv=\pm\square_k$ より $N_{k/\mathbb{Q}}(v)=1$ である. (1) のノルムを考えて,

$$N_{k/\mathbb{Q}}(X)^3=N_{k/\mathbb{Q}}(u)+27\,\mathrm{Tr}_{k/\mathbb{Q}}(u'v)+729N_{k/\mathbb{Q}}(v)=730+27\,\mathrm{Tr}_{k/\mathbb{Q}}(u'v)\tag{8}$$

を得る.[4] 仮定より $u'v=u^{-1}v=uv/u^2=\pm w^2$ である $w\in\mathcal{O}_k^{\times}$ が存在するので,

$$\mathrm{Tr}_{k/\mathbb{Q}}(u'v)=\pm\,\mathrm{Tr}_{k/\mathbb{Q}}(w^2)=\pm\{\mathrm{Tr}_{k/\mathbb{Q}}(w)^2-2N_{k/\mathbb{Q}}(w)\}$$

が成り立ち,

$$\begin{aligned}N_{k/\mathbb{Q}}(X)^3&=730\pm 27\{\mathrm{Tr}_{k/\mathbb{Q}}(w)^2-2N_{k/\mathbb{Q}}(w)\}\\&=\pm 27\,\mathrm{Tr}_{K/\mathbb{Q}}(w)^2+730\mp 54N_{k/\mathbb{Q}}(w)\end{aligned}$$

が得られる. (複号は $u'v=\pm w^2$ と同順.)

$u'v=w^2$ とすると,

$$27\,\mathrm{Tr}_{k/\mathbb{Q}}(w)^2=\begin{cases}N_{k/\mathbb{Q}}(X)^3-676 & (N_{k/\mathbb{Q}}(w)=1\text{ の時})\\ N_{k/\mathbb{Q}}(X)^3-784 & (N_{k/\mathbb{Q}}(w)=-1\text{ の時})\end{cases}$$

であり, $27y^2=x^3-676$ を満たす $x,y\in\mathbb{Z}$ は無く ($x,y\in\mathbb{Q}$ も無い), $27y^2=x^3-784$ の整数点は $(x,y)=(19,\pm 15)$, $(28,\pm 28)$ のみである. (SageMath を使って確認出来る.) よって $N_{k/\mathbb{Q}}(w)=-1$, $\mathrm{Tr}_{k/\mathbb{Q}}(w)=\pm 15,\ \pm 28$, 即ち $w=\pm(15\pm\sqrt{229})/2,\ \pm(14\pm\sqrt{197})$ である. $w=\pm(15\pm\sqrt{229})/2$ の時は $(u+27v)=\mathfrak{p}_{19}^3$ ($\mathfrak{p}_{19}$ は 19 を割る素イデアル) であるが, $\mathfrak{p}_{19}$ は単項イデアルでないので不適. ($h_{\mathbb{Q}(\sqrt{229})}=3$ である.) $w=\pm(14\pm\sqrt{197})$ の時は $(u+27v)=(2)^3\mathfrak{p}_7^2\mathfrak{p}_7'$, $\mathfrak{p}_7\mathfrak{p}_7'=(7)$, $\mathfrak{p}_7\neq\mathfrak{p}_7'$ であるので不適.

$u'v=-w^2$ とすると,

$$-27\,\mathrm{Tr}_{k/\mathbb{Q}}(w)^2=\begin{cases}N_{k/\mathbb{Q}}(X)^3-676 & (N_{k/\mathbb{Q}}(w)=-1\text{ の時})\\ N_{k/\mathbb{Q}}(X)^3-784 & (N_{k/\mathbb{Q}}(w)=1\text{ の時})\end{cases}$$

であり, $-27y^2=x^3-784$ を満たす $x,y\in\mathbb{Z}$ は無く ($x,y\in\mathbb{Q}$ も無い), $-27y^2=x^3-676$ の整数点は $(x,y)=(1,\pm 5)$, $(-26,\pm 26)$ のみである. よって $N_{k/\mathbb{Q}}(w)=-1$, $\mathrm{Tr}_{k/\mathbb{Q}}(w)=\pm 5,\pm 26$, 即ち $w=\pm(5\pm\sqrt{29})/2,\pm(13\pm\sqrt{170})$. $w=\pm(13\pm\sqrt{170})$ の時は $(u+27v)=\mathfrak{p}_2^3\mathfrak{p}_{13}^2\mathfrak{p}_{13}'$,

[4] 二次体の元 x に対し, その共役を x' と書くことにする.

$(2)=\mathfrak{p}_2^2$, $(13)=\mathfrak{p}_{13}\mathfrak{p}'_{13}$, $\mathfrak{p}_{13}\neq\mathfrak{p}'_{13}$ であるので不適. $w=\pm(5\pm\sqrt{29})/2=\pm\varepsilon_{29},\pm\varepsilon'_{29}$ の時は, $v=-\varepsilon_{29}^2u$ または $v=-\varepsilon_{29}^{-2}u$ であり, $u+27v=-\varepsilon_{29}^4u$ または $u+27v=-\varepsilon_{29}^{-4}u$ である. $X^3=u+27v$ が 3 乗数であることにより, $u=\pm\varepsilon_{29}^{3n+4},\pm\varepsilon_{29}^{3n-4}$ である $n\in\mathbb{Z}$ が存在し, $X=\mp\varepsilon_{29}^n$ である. □

注意. [15] で次のことが示されている: $m\in\mathbb{Z}$, $X\in\mathcal{O}_{\mathbb{Q}(\sqrt{29})}$ に対し,

$$X^3=\varepsilon_{29}^{4+12m}-27\varepsilon_{29}^2\iff m=0,\ X=-1.$$

定理 3.2 はこれの一般化に成っている.[5]

定理 3.3 ([11])**.** p を $p=2$ または $p\neq3$, $p\equiv3\pmod4$ なる素数とし, $k:=\mathbb{Q}(\sqrt{3p})$ とする. (1) が解を持つのは $p=2$ または $p=11$ (即ち $k=\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{33})$) の時のみで, 解は $(X,u,v)=((4+\sqrt{6})\varepsilon_6^n,\varepsilon_6^{3n},\varepsilon_6^{3n+1})$, $((4-\sqrt{6})\varepsilon_6^n,\varepsilon_6^{3n},\varepsilon_6^{3n-1})$, $((-5-\sqrt{33})\varepsilon_{33}^n,\varepsilon_{33}^{3n},-\varepsilon_{33}^{3n+1})$, $((-5+\sqrt{33})\varepsilon_{33}^n,\varepsilon_{33}^{3n},-\varepsilon_{33}^{3n-1})$ のみである. ここで $n\in\mathbb{Z}$ は任意で, $\varepsilon_6=5+2\sqrt{6}$, $\varepsilon_{33}=23+4\sqrt{33}$ はそれぞれ $\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{33})$ の基本単数である.[6]

証明. 解があるとする. 仮定の下で全ての単数のノルムは 1 なので, (1) のノルムをとり (8) が得られる. $uv=\pm\square_k$ の場合は定理 3.2 で済んでいるので, $uv\neq\pm\square_k$ とする. この時 $u'v=u^{-1}v=\pm\varepsilon w^2$ である $w\in\mathcal{O}_k^\times$ が存在する. 3 は k で分岐していて, h_k は奇数である[7]から, $(3)=(\pi^2)$ である $\pi\in\mathcal{O}_k$ が存在する. $\pi^2/3>0$ で $k\neq\mathbb{Q}(\sqrt{3})$ であるから, $3\varepsilon=(\pi\varepsilon^n)^2$ である $n\in\mathbb{Z}$ が存在する. よって $\sqrt{3\varepsilon}=\pi\varepsilon^n\in\mathcal{O}_k$ であるので,

$$\begin{aligned}27\operatorname{Tr}_{k/\mathbb{Q}}(u'v)&=\pm27\operatorname{Tr}_{k/\mathbb{Q}}(\varepsilon w^2)\\&=\pm9\operatorname{Tr}_{k/\mathbb{Q}}((\sqrt{3\varepsilon}\,w)^2)\\&=\pm9\{\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)^2-2N_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)\}\\&=\pm9\{\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)^2-2N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})\}\end{aligned}$$

が得られる. (複号は $u'v=\pm\varepsilon w^2$ と同順.) よって

$$N_{k/\mathbb{Q}}(X)^3=\begin{cases}730+9\{\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)^2-2N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})\}&(u'v=\varepsilon w^2\text{ の時})\\730-9\{\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)^2-2N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})\}&(u'v=-\varepsilon w^2\text{ の時}),\end{cases}$$

$u'v=\varepsilon w^2$ の時

$$\{3\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)\}^2=\begin{cases}N_{k/\mathbb{Q}}(X)^3-676&(N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})=3\text{ の時})\\N_{k/\mathbb{Q}}(X)^3-784&(N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})=-3\text{ の時}),\end{cases}$$

$u'v=-\varepsilon w^2$ の時

$$\{3\operatorname{Tr}_{k/\mathbb{Q}}(\sqrt{3\varepsilon}\,w)\}^2=\begin{cases}\{-N_{k/\mathbb{Q}}(X)\}^3+784&(N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})=3\text{ の時})\\\{-N_{k/\mathbb{Q}}(X)\}^3+676&(N_{k/\mathbb{Q}}(\sqrt{3\varepsilon})=-3\text{ の時})\end{cases}$$

[5] 正直, [15] の証明が理解出来ないので, 適当にノルムを考えたらうまいこと定理 3.2 が得られたのであるが.
[6] 定理 3.1 と同じ解である.
[7] 実二次体 k の類数が奇数 $\iff$ $k=\mathbb{Q}(\sqrt{p})$ (p は素数), $\mathbb{Q}(\sqrt{2p})$ (p は素数で $p\equiv3\pmod4$), $\mathbb{Q}(\sqrt{pq})$ (p,q は異なる $p,q\equiv3\pmod4$ なる素数).

なので, 楕円曲線 $y^2 = x^3 \pm 784$, $y^2 = x^3 \pm 676$ の整数点を求めることに帰着された. $y^2 = x^3 - 784$ を満たす $x, y \in \mathbb{Z}$ は無く ($x, y \in \mathbb{Q}$ も無い), $y^2 = x^3 + 676$ を満たす $x, y \in \mathbb{Z}$ は $(x, y) = (0, \pm 26)$ のみ ($(x, y) \in \mathbb{Q} \times \mathbb{Q}$ もこの二つだけ), $y^2 = x^3 - 676$ を満たす $x, y \in \mathbb{Z}$ は $(x, y) = (10, \pm 18)$, $(13, \pm 39)$, $(26, \pm 130)$, $(130, \pm 1482)$, $(338, \pm 6214)$, $(901, \pm 27045)$ のみ, $y^2 = x^3 + 784$ を満たす $x, y \in \mathbb{Z}$ は $(x, y) = (-7, \pm 21)$, $(0, \pm 28)$, $(8, \pm 36)$, $(56, \pm 420)$ のみであることが SageMath を使って確認出来る. この後計算 (ちょと嫌な計算) すると, 主張にあるような解しか出て来ないことが示せる. 詳細は [9] を参照あれ. □

定理 3.4 ([12])**.** k を実二次体とする. (1) の解で v が 3 乗数であるものは無い.[8]

証明. 解があるとする. 必要なら (1) の両辺に 3 乗数を掛けて, $v = 1$ としてよい. この時 $u = (X - 3)(X^3 + 3X + 9)$ だから, $X - 3 =: v_1 \in \mathcal{O}_k^\times$, $X^2 + 3X + 9 =: v_2 \in \mathcal{O}_k^\times$ である. X を消去して, $v_2 = v_1^2 + 9v_1 + 27$ が得られる. これのノルムをとって,

$$N_{k/\mathbb{Q}}(v_2) = 27\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + 9\{N_{k/\mathbb{Q}}(v_1) + 27\}\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 729 + 27N_{k/\mathbb{Q}}(v_1) + 1$$

を得る. 右辺は 3 を法として 1 と合同なので, $N_{k/\mathbb{Q}}(v_2) = 1$ でなくてはならない. よって

$$3\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2 + \{N_{k/\mathbb{Q}}(v_1) + 27\}\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1) + 81 + 3N_{k/\mathbb{Q}}(v_1) = 0. \tag{9}$$

2 次式 $3x^2 + \{N_{k/\mathbb{Q}}(v_1) + 27\}x + 81 + 3N_{k/\mathbb{Q}}(v_1)$ の判別式は, $N_{k/\mathbb{Q}}(v_1) = 1$ の時は $-224 < 0$, $N_{k/\mathbb{Q}}(v_1) = -1$ の時は $-260 < 0$ なので, (9) は成り立たない. □

定理 3.5 ([12])**.** k を実二次体とする. (1) が $X \in \mathcal{O}_k^\times$ である解を持つのは $k = \mathbb{Q}(\sqrt{29})$, $\mathbb{Q}(\sqrt{733})$ の時のみで, $k = \mathbb{Q}(\sqrt{29})$ の時は解は

$$(X, u, v) = (\pm\varepsilon_{29}^n, \mp\varepsilon_{29}^{3n-4}, \pm\varepsilon_{29}^{3n-2}), (\pm\varepsilon_{29}^n, \mp\varepsilon_{29}^{3n+4}, \pm\varepsilon_{29}^{3n+2}),$$

$k = \mathbb{Q}(\sqrt{733})$ の時は解は

$$(X, u, v) = (\pm\varepsilon_{733}^n, \pm\varepsilon_{733}^{3n-2}, \pm\varepsilon_{733}^{3n-1}), (\pm\varepsilon_{733}^n, \pm\varepsilon_{733}^{3n+2}, \mp\varepsilon_{733}^{3n+1}).$$

ここで $n \in \mathbb{Z}$ は任意で, $\varepsilon_{29} = (5+\sqrt{29})/2$, $\varepsilon_{733} = (27+\sqrt{733})/2$ はそれぞれ $\mathbb{Q}(\sqrt{29})$, $\mathbb{Q}(\sqrt{733})$ の基本単数である.

証明. 解があるとする. (1) に 3 乗数を掛けたり (1) の共役を考えることによって, $v = 1, \varepsilon$ としてよい (ε (> 1) は k の基本単数). 定理 3.4 より $v = \varepsilon$ である. $X^3 = u + 27\varepsilon$ のノルムをとると, $N_{k/\mathbb{Q}}(X)^3 = N_{k/\mathbb{Q}}(u) + 27\,\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon' u) + 729N_{k/\mathbb{Q}}(\varepsilon)$. $N_{k/\mathbb{Q}}(X) = \pm 1$, $N_{k/\mathbb{Q}}(u) = \pm 1$ なので, 3 を法として考えることにより $N_{k/\mathbb{Q}}(X)^3 = N_{k/\mathbb{Q}}(u)$ が分かる. よって $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon' u) = -27N_{k/\mathbb{Q}}(\varepsilon)$ である.

$N_{k/\mathbb{Q}}(\varepsilon) = -1$ とする. $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon' u) = 27$, $N_{k/\mathbb{Q}}(\varepsilon' u) = -N_{k/\mathbb{Q}}(u)$ だから, $\varepsilon' u$ は 2 次式 $x^2 - 27x - N_{k/\mathbb{Q}}(u)$ の根である. よって

$$\varepsilon' u = \begin{cases} (27 \pm \sqrt{733})/2 & (N_{k/\mathbb{Q}}(u) = 1 \text{ の時}) \\ (27 \pm 5\sqrt{29})/2 & (N_{k/\mathbb{Q}}(u) = -1 \text{ の時}) \end{cases}$$

[8] (1) に関して最初に得られていたのが定理 3.4 と定理 3.5 である.

が得られるので $k=\mathbb{Q}(\sqrt{29}),\mathbb{Q}(\sqrt{733})$ で,

$$u=\begin{cases}-\varepsilon_{733}^2,1 & (N_{k/\mathbb{Q}}(u)=1\text{ の時})\\ -\varepsilon_{29}^3,-\varepsilon_{29}^{-1} & (N_{k/\mathbb{Q}}(u)=-1\text{ の時}).\end{cases}$$

$k=\mathbb{Q}(\sqrt{733})$ の時の $u=1$ と $k=\mathbb{Q}(\sqrt{29})$ の時の $u=-\varepsilon_{29}^3$ は定理 3.1 より不適[9]で, $-\varepsilon_{733}^2+27\varepsilon_{733}=(-1)^3$, $-\varepsilon_{29}^{-1}+27\varepsilon_{29}=\varepsilon_{29}^3$ である.

$N_{k/\mathbb{Q}}(\varepsilon)=1$ とする. $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon' u)=-27$, $N_{k/\mathbb{Q}}(\varepsilon' u)=N_{k/\mathbb{Q}}(u)$ だから, $\varepsilon' u$ は 2 次式 $x^2+27x+N_{k/\mathbb{Q}}(u)$ の根である. よって $\varepsilon' u=(-27\pm\sqrt{733})/2,(-27\pm5\sqrt{29})/2$ なので $k=\mathbb{Q}(\sqrt{29}),\mathbb{Q}(\sqrt{733})$ であるが, $\varepsilon_{29},\varepsilon_{733}$ のノルムはどちらも -1 なので不適である. □

コンピューターを走らせた結果を見ると, 次のことが予想出来る:

予想 1. k を実二次体とする. (1) が解を持つのは $k=\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{29}),\mathbb{Q}(\sqrt{33}),\mathbb{Q}(\sqrt{733})$ の時のみ.

問. 予想 1 を証明せよ.

問. $k=\mathbb{Q}(\sqrt{29}),\mathbb{Q}(\sqrt{733})$ の時に (1) の解を完全に決定せよ. (完全に解けているのは定理 3.3 の時のみなので.)

4 $X^3=u+v$

次に (2) に関する結果を挙げる.[10] k を実二次体とする. (2) に 3 乗数を掛けたり (2) の共役を考えることによって, $u=1,\varepsilon$ としてよい (ε (>1) は k の基本単数).

定理 4.1 ([11])**.** k を実二次体とする. $X^3=1+v$ を満たす $X\in\mathcal{O}_k-\{0\}$, $v\in\mathcal{O}_k^\times$ は無い.

証明. $(X-1)(X^2+X+1)=v\in\mathcal{O}_k^\times$ だから, $X-1=:v_1\in\mathcal{O}_k^\times$, $X^2+X+1=:v_2\in\mathcal{O}_k^\times$ である. X を消去して $v_1^2+3v_1+3=v_2$ が得られる. これのノルムをとって,

$$N_{k/\mathbb{Q}}(v_2)=3\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2+3\{N_{k/\mathbb{Q}}(v_1)+3\}\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)+9+3N_{k/\mathbb{Q}}(v_1)+1$$

を得る. 右辺は 3 を法として 1 と合同なので, $N_{k/\mathbb{Q}}(v_2)=1$ でなくてはならない. よって

$$\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2+\{N_{k/\mathbb{Q}}(v_1)+3\}\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)+3+N_{k/\mathbb{Q}}(v_1)=0.$$

$N_{k/\mathbb{Q}}(v_1)=-1$ ならば $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2+2\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)+2=0$ が得られるが, $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)\in\mathbb{Z}$ なのでこれは不可能. $N_{k/\mathbb{Q}}(v_1)=1$ ならば $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)^2+4\,\mathrm{Tr}_{k/\mathbb{Q}}(v_1)+4=0$ となるので, $\mathrm{Tr}_{k/\mathbb{Q}}(v_1)=-2$. 故に $v_1=-1$, $X=0$ である. □

よって

$$X^3=\varepsilon+v,\quad X\in\mathcal{O}_k-\{0\},\quad v\in\mathcal{O}_k^\times \tag{10}$$

を考える.

定理 4.2. ε のノルムが 1 の時, (10) の解で $v=-\varepsilon^{2n+1}$ ($n\in\mathbb{Z}$) であるものは無い.

[9] $1+27\varepsilon_{733}=\varepsilon_{733}^2$, $-\varepsilon_{29}^3+27\varepsilon_{29}=\varepsilon_{29}^{-1}$ はどちらも 3 乗数でない, としてもよい.
[10] (1) より (2) の方が色々面白いので, そっちばっかりいじってるのが現状である.

証明. 解があるとする. ノルムをとって, $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^n)^2 = \{-N_{k/\mathbb{Q}}(X)\}^3 + 4$ が得られる. [1] に依れば, $y^2 = x^3 + 4$ (108A1 というラベルが振られている) を満たす $x, y \in \mathbb{Q}$ は $x = 0, y = \pm 2$ のみである. 故に $X = 0$ なので不適である. □

$X^3 = \varepsilon + \varepsilon^{2n+1}$ だと $N_{k/\mathbb{Q}}(X)^3 = \mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^n)^2$ となり, 特異点を持つ 3 次曲線 $y^2 = x^3$ の整数点問題に成るのでうまくいかない. しかし 2 乗して 3 乗数なのだから, $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^n)$ は 3 乗数である. こういったことを考慮して色々やって (と一言で済むほど簡単なことでは無いが), 次の定理が示せた:

定理 4.3 ([10])**.** p を $p \neq 3$, $p \equiv 3 \pmod 4$ なる素数とし, $k := \mathbb{Q}(\sqrt{3p})$ とおく. (10) の解 X, v が存在するとする.

(i) $p \equiv 1 \pmod 3$ ならば,

- $v = -\varepsilon^{6n+2}$ となる $n \in \mathbb{Z}$ が存在する.
- $\varepsilon^{6n+1} = (a + b\sqrt{3p})/2$ $(a, b \in \mathbb{N})$, $c = N_{k/\mathbb{Q}}(X)$ とすると, $c^3 = 2 - a = -3\square_{\mathbb{Q}}$ が成り立ち, c は奇数である.
- $3pb^2 = c^6 - 4c^3 = a^2 - 4$, $c^3 - 4 = -p\square_{\mathbb{Q}}$ が成り立つ.
- $p \equiv 7 \pmod 8$ である.

(ii) $p \equiv 2 \pmod 3$ ならば,

- $v = \varepsilon^{6n+2}$ となる $n \in \mathbb{Z}$ が存在する.
- $\varepsilon^{6n+1} = (a + b\sqrt{3p})/2$ $(a, b \in \mathbb{N})$, $c = N_{k/\mathbb{Q}}(X)$ とすると, $c^3 = a + 2 = 3\square_{\mathbb{Q}}$, $3pb^2 = c^6 - 4c^3 = a^2 - 4$, $c^3 - 4 = p\square_{\mathbb{Q}}$ が成り立つ.
- $p \equiv 7 \pmod 8$ である.

系 4.4. p を $p \neq 3$, $p \equiv 3 \pmod 8$ なる素数とし, $k := \mathbb{Q}(\sqrt{3p})$ とおく. この時 (10) は解無し. (故に (2) は解無し.)

定理 4.3 により (10) の解き方が分かる. 例を 2 つ挙げる.

例 4.5. $p = 23$ $(\equiv 7 \pmod 8, \equiv 2 \pmod 3)$ とする. 定理 4.3, (ii) より, $v = \varepsilon^{6n+2}$ となる $n \in \mathbb{Z}$ が存在する. $a, b \in \mathbb{N}$, $c \in \mathbb{Z}$ を定理 4.3, (ii) の通りとすると,

$$c^3 = a + 2 = 3\square_{\mathbb{Q}}, \quad 69b^2 = c^6 - 4c^3 = a^2 - 4, \quad c^3 - 4 = 23\square_{\mathbb{Q}}.$$

SageMath によれば $23y^2 = x^3 - 4$ の整数点は $(x, y) = (3, \pm 1)$ のみ. よって $c = 3$, $a = c^3 - 2 = 25$, $b^2 = (a^2 - 4)/69 = 3^2$, $\varepsilon_{23}^{6n+1} = (a + b\sqrt{3p})/2 = (25 + 3\sqrt{69})/2 = \varepsilon_{23}$, $X^3 = \varepsilon_{23} + \varepsilon_{23}^2 = ((9 + \sqrt{69})/2)^3$. 故に解は $(X, v) = ((9 + \sqrt{69})/2, \varepsilon_{23}^2)$ のみである.

例 4.6. $p = 263$ $(\equiv 7 \pmod 8, \equiv 2 \pmod 3)$ とする. (10) に解があるとする. $c \in \mathbb{Z}$ を定理 4.3, (ii) の通りとすると, $c = 3\square_{\mathbb{Q}}$, $c^3 - 4 = 263\square_{\mathbb{Q}}$. SageMath によれば $263y^2 = x^3 - 4$ の整数点は $(x, y) = (96, \pm 58)$ のみなので $c = 96$ でなくてはいけないが, $96 = 2^5 \times 3 \neq 3\square_{\mathbb{Q}}$ なので不適である. よって (10) は解無し. (故に (2) は解無し.)

もっと簡単に解が無いことを示せないか？と考え, 次の定理を証明した.

定理 4.7 ([11])**.** p を $p \equiv 7 \pmod 8$ である素数とし, $k := \mathbb{Q}(\sqrt{3p})$ とおく. $\varepsilon\ (>1)$ を k の基本単数とする.

(i) $p \equiv 1 \pmod 3$ の時, $\mathrm{ord}_3(\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon) - 2) \not\equiv 0 \pmod 3$ ならば (10) は解無し (よって (2) は解無し).

(ii) $p \equiv 2 \pmod 3$ の時, $\mathrm{ord}_3(\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon) + 2) \not\equiv 0 \pmod 3$ ならば (10) は解無し (よって (2) は解無し).

例 4.8. $p = 263\ (\equiv 7 \pmod 8,\ \equiv 2 \pmod 3)$ とする. $k := \mathbb{Q}(\sqrt{3p})$ の基本単数は $\varepsilon = (31825 + 1133\sqrt{789})/2$. $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon) + 2 = 3 \times 103^2$ なので, $\mathrm{ord}_3(\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)+2) = 1 \not\equiv 0 \pmod 3$. 故に (2) は解無し.

定理 4.3 を使って得られる非存在を示す規準を二つ与える (定理 4.11, 定理 4.13, 未発表).

補題 4.9. p を $p \equiv 3 \pmod 4$ なる素数とする. $3 \nmid h_{\mathbb{Q}(\sqrt{-p})}$ とすると, $py^2 = x^3 - 4$ を満たす奇数 $x, y \in \mathbb{Z}$ は存在しない.

証明. $3y^2 = x^3 - 4$ を満たす $x, y \in \mathbb{Q}$ は無い (これは [1] の表の曲線 108A2 と $\mathbb{Q}$ 上同型である) ので, $p \neq 3$ とする. $x^3 = 4 + py^2 = (2 + y\sqrt{-p})(2 - y\sqrt{-p})$ と分解して, $\mathbb{Q}(\sqrt{-p})$ で考える. y が奇数であることを用いると, 単項イデアル $(2 + y\sqrt{-p})$, $(2 - y\sqrt{-p})$ が互いに素であることが容易に分かるので, $(2 + y\sqrt{-p}) = \mathfrak{a}^3$ である $\mathbb{Q}(\sqrt{-p})$ の整イデアル $\mathfrak{a}$ が存在する. よって $3 \nmid h_{\mathbb{Q}(\sqrt{-p})}$, $-p \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{-p}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ より, $a, b \in \mathbb{Z}$ で, $a \equiv b \pmod 2$ かつ

$$2 + y\sqrt{-p} = \left(\frac{a + b\sqrt{-p}}{2}\right)^3$$

であるものが存在することが分かる. 右辺を展開して両辺の実部を比べれば, $16 = a(a^2 - 3pb^2)$ が得られるが, これを満たす a, b が無いことは容易に分かる. □

注意. (1) $p = 127$ の時 $h_{\mathbb{Q}(\sqrt{-p})} = 5$ で, $py^2 = 127y^2 = x^3 - 4$ は解 $(x, y) = (8, \pm 2)$ を持つ. (整数点はこれだけである.) よって偶数解が存在することがある.

(2) $p = 23$ の時 $h_{\mathbb{Q}(\sqrt{-p})} = 3$ で, $py^2 = 23y^2 = x^3 - 4$ は解 $(x, y) = (3, \pm 1)$ を持つ. (整数点はこれだけである.) よって $3 \mid h_{\mathbb{Q}(\sqrt{-p})}$ なら奇数解を持つことはあるので, 仮定 $3 \nmid h_{\mathbb{Q}(\sqrt{-p})}$ は必要.

補題 4.10. $k = \mathbb{Q}(\sqrt{m})$ を実二次体 ($m\ (>1)$ は square-free), $\varepsilon\ (>1)$ を k の基本単数とする.

(i) $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)$ が奇数なら $m \equiv 5 \pmod 8$ である.

(ii) $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)$ が奇数の時, $n \in \mathbb{Z}$ に対し, $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^n)$ が偶数 $\iff 3 \mid n$.

証明. (i) $\varepsilon = (a + b\sqrt{m})/2$, $a\ (= \mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon))$, b を奇数とすると, $a^2 - mb^2 = \pm 4$ なので, $m \equiv mb^2 = a^2 \mp 4 \equiv 5 \pmod 8$ である.

(ii) $u \in \mathcal{O}_k^\times$ に対し,「$u \equiv 1 \pmod 2 \iff \mathrm{Tr}_{k/\mathbb{Q}}(u)$ が偶数」が容易にわかる. このことと $(\mathcal{O}_k/(2))^\times = \mathbb{F}_4^\times$ が位数 3 の巡回群であることから主張が従う. □

定理 4.11. p を $p \equiv 7 \pmod 8$, $p \equiv 2 \pmod 3$ なる素数とし, $k := \mathbb{Q}(\sqrt{3p})$ とおく. $\varepsilon\ (>1)$ を k の基本単数とする. $\mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon)$ が奇数で $3 \nmid h_{\mathbb{Q}(\sqrt{-p})}$ ならば (10) は解無し (故に (2) は解無し).[11]

[11] ちょっと分かりづらいが, 類数の仮定は $\mathbb{Q}(\sqrt{-p})$ に対してで, 解の有無は $\mathbb{Q}(\sqrt{3p})$ で考えている.

証明. (10) が解を持つとすると, 定理 4.3, (ii) より, $v = \varepsilon^{6n+2}$ となる $n \in \mathbb{Z}$ が存在する. $\varepsilon^{6n+1} = (a+b\sqrt{3p})/2, a, b \in \mathbb{N}$ とすると, $3 \nmid (6n+1)$ なので, 補題 4.10 より $a = \mathrm{Tr}_{k/\mathbb{Q}}(\varepsilon^{6n+1})$ は奇数である. $c := N_{K/\mathbb{Q}}(X)$ とすると, 再び定理 4.3, (ii) より $c^3 = a+2$ は奇数で, $c^3 - 4 = p\square_{\mathbb{Q}}$. これは補題 4.9 より不可能. □

例 4.12. $p = 71$ の時, $h_{\mathbb{Q}(\sqrt{-p})} = 7$ で, $k = \mathbb{Q}(\sqrt{3p}) = \mathbb{Q}(\sqrt{213})$ の基本単数は $(73+5\sqrt{213})/2$ である. 故に (2) の解は無い.

定理 4.13. p を $p \equiv 7 \pmod 8$, $p \equiv 1 \pmod 3$ なる素数とする. $2^{(p-1)/3} \not\equiv 1 \pmod p$ ならば (10) は $\mathbb{Q}(\sqrt{3p})$ に解を持たない. (従って (2) は解無し.)

証明. (10) が解を持つとする. $c := N_{k/\mathbb{Q}}(X)$ とすると, 定理 4.3, (i) より $c^3 - 4 = p\square_{\mathbb{Q}}$ が成り立つ. よって $c^3 \equiv 4 \pmod p$ が成り立つので, $x^3 \equiv 2 \pmod p$ なる $x \in \mathbb{Z}$ が存在する. 初等整数論よりこれは $2^{(p-1)/3} \equiv 1 \pmod p$ と同値. □

これで暫く止まっていたが, 学生に [2] を読んでもらっている時に次の補題の存在を知った:

補題 4.14 ([2], Proposition 9.6.2)**.** p が $p \equiv 1 \pmod 3$ なる素数の時,

$$\begin{aligned} &\text{合同式 } x^3 \equiv 2 \pmod p \text{ が解 } x \in \mathbb{Z} \text{ を持つ} \\ &\quad \Longleftrightarrow\ p = C^2 + 27D^2 \text{ となる } C, D \in \mathbb{N} \text{ が存在する.} \end{aligned}$$

よって C, D を走らせれば素数 $p = C^2 + 27D^2$ で, (10) が解を持つ新しい p の例が沢山見付けられるのでは？と思って $C, D \le 300$ で探したが, 見付かったのは

$$\begin{aligned} 31 &= 2^2 + 27 \times 1^2, & \left(-\frac{9+3\sqrt{93}}{2}\right)^3 &= \varepsilon - \varepsilon^2, \\ 439 &= 14^2 + 27 \times 3^2, & \left(-\frac{5625+155\sqrt{1317}}{2}\right)^3 &= \varepsilon - \varepsilon^2, \\ 19687 &= 2^2 + 27 \times 27^2, & \left(-\frac{729+3\sqrt{59061}}{2}\right)^3 &= \varepsilon - \varepsilon^2 \end{aligned}$$

だけであった. $p = 31, 439$ の時は大分前に見付けていて, もっと新しい例が沢山欲しかった. 残念ではあったが, まあ新しい例 19687 が見付かったのでいいです.

コンピューターを走らせて数表を作った結果を見ると, 次のことが予想出来る:

予想 2. k を実二次体とする. (10) の解は $k \neq \mathbb{Q}(\sqrt{5})$ なら高々一つであり, $k \neq \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{29})$ なら, v は $\pm\varepsilon^{-1}$, $\pm\varepsilon^2$ のどれかである.

$\mathbb{Q}(\sqrt{5})$ では解が四つ見付かっている:

$$1^3 = \varepsilon_5 - \varepsilon_5^{-1}, \quad (-1)^3 = \varepsilon_5 - \varepsilon_5^2, \quad \varepsilon_5^3 = \varepsilon_5 + \varepsilon_5^2, \quad (\sqrt{5}\,\varepsilon_5^2)^3 = \varepsilon_5 + \varepsilon_5^{11}.$$

ここで $\varepsilon_5 = (1+\sqrt{5})/2$ は $\mathbb{Q}(\sqrt{5})$ の基本単数. 最初の三つは ε_5 が満たす自明な関係式 $\varepsilon_5^2 - \varepsilon_5 - 1 = 0$ の書き換えに過ぎないので, 非自明なのは四つ目のものだけである. $\mathbb{Q}(\sqrt{29})$ では $(3\varepsilon_{29})^3 = \varepsilon_{29} + \varepsilon_{29}^5$ という解が見付かっている. ここで $\varepsilon_{29} = (5+\sqrt{29})/2$ は $\mathbb{Q}(\sqrt{29})$ の基本単数. これは $\mathrm{Tr}_{\mathbb{Q}(\sqrt{29})/\mathbb{Q}}(\varepsilon_{29}^2) = 3^3$ の言い換えに過ぎない.[12]

上の二つの場合は次が成り立つことが示せた:

[12] k が二次体の時, $\mathrm{Tr}_{k/\mathbb{Q}}(w^2) = x^3$ である $w \in \mathcal{O}_k^\times$, $x \in \mathbb{Z}$ が存在するのは $k = \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{29})$ の時のみで, $k = \mathbb{Q}(\sqrt{-3})$ の時は $w = (\pm 1 \pm \sqrt{-3})$, $x = -1$ のみ, $k = \mathbb{Q}(\sqrt{29})$ の時は $w = (\pm 5 \pm \sqrt{29})/2$, $x = 3$ のみであることが証明出来る. ($y^2 = x^3 \pm 2$ の整数点を決定する必要がある. SageMath を使えばよい.)

定理 4.15. (i) $k=\mathbb{Q}(\sqrt{5})$ の時, (10) の解は

$$(X,v)=(1,-\varepsilon_5^{-1}),(-1,-\varepsilon_5^2),(\varepsilon_5,\varepsilon_5^2),(\sqrt{5}\,\varepsilon_5^2,\varepsilon_5^{11})$$

の丁度四つである.

(ii) $k=\mathbb{Q}(\sqrt{29})$ の時, (10) の解は $(X,v)=(3\varepsilon_{29},\varepsilon_{29}^5)$ のみである.

k が定理 4.3 にあるような実二次体の場合, 解が高々一つというだけなく, もう少し詳しいことが成り立つであろうと予想出来る:

予想 3. p を $p\equiv 7 \pmod 8$ なる素数とし, $k:=\mathbb{Q}(\sqrt{3p})$ とおく. (10) の解は高々一つで, 解がある時は

$$v=\begin{cases}-\varepsilon^2 & (p\equiv 1 \pmod 3 \text{ の時})\\ +\varepsilon^2 & (p\equiv 2 \pmod 3 \text{ の時})\end{cases}$$

のみである.

$3<p<5000$ の範囲で予想 3 は正しい, と大袈裟に言いたいが, $p\equiv 1 \pmod 3$ の時は $p=31, 439$ の時に解は $v=-\varepsilon^2$ のみ, $p\equiv 2 \pmod 3$ の時は $p=23, 431$ の時に解は $v=\varepsilon^2$ のみ, これ以外の p に対しては解が無い, というのが本当のところである.

問. 予想 2, 予想 3 を証明せよ.

5 EGR を持つ楕円曲線に関する結果

(1), (2) を使って得られている EGR を持つ楕円曲線に関する結果を挙げておく.

次の結果が必要になる:

補題 5.1 ([13])**.** k を二次体とし, $j\in\mathcal{O}_k$ とする. k 上 EGR を持ち j 不変量が j である楕円曲線が存在するとする. この時そのような楕円曲線の k 上の同型類の個数は 2^{t-1} である. ここで t は k で分岐する素数の個数である.

定理 5.2 ([6])**.** p を $p=2$ または $p\neq 3$, $p\equiv 3 \pmod 4$ なる素数とし, $k:=\mathbb{Q}(\sqrt{3p})$ とおく. この時 k 上 EGR を持ち判別式が 3 乗数である楕円曲線が存在するのは $p=2,11$, 即ち $k=\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{33})$ の時のみで, $k=\mathbb{Q}(\sqrt{6})$ の時はそのような楕円曲線は

$$E_1: y^2+(4+\sqrt{6})xy+\varepsilon_6 y=x^3,\quad \Delta(E_1)=\varepsilon_6^3,\quad j(E_1)=8000,$$

もしくは E_1 の共役 E_1' と $\mathbb{Q}(\sqrt{6})$ 上同型, $k=\mathbb{Q}(\sqrt{33})$ の時は

$$E_2: y^2+(5+\sqrt{33})xy+\varepsilon_{33} y=x^3,\quad \Delta(E_2)=-\varepsilon_{33}^3,\quad j(E_2)=-32768,$$

もしくは E_2 の共役 E_2' と $\mathbb{Q}(\sqrt{33})$ 上同型. ここで $\varepsilon_6=5+2\sqrt{6}$, $\varepsilon_{33}=23+4\sqrt{33}$ はそれぞれ $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{33})$ の基本単数である.

証明. $k=\mathbb{Q}(\sqrt{6})$ の時は, k 上 EGR を持つ楕円曲線は決定されていて, 判別式が 3 乗数のものは E_1, E_1' のみである. ([5] を見よ.) $p\neq 2$ とする. 主張にあるような楕円曲線 E が存在するとせよ.

$$h_{k(\sqrt{-3})}((\sqrt{-3}))=\begin{cases}2h_{k(\sqrt{-3})} & (p\equiv 1 \pmod 3 \text{ の時})\\ h_{k(\sqrt{-3})} & (p\equiv 2 \pmod 3 \text{ の時})\end{cases}$$

であり, $h_{k(\sqrt{-3})}$ は奇数である. よって定理 2.5 の仮定が満たされるので, E から他の楕円曲線への k 上定義された 3 次の isogeny がある. 従って $j(E)=J(t)$, $(t)=(1)$, (3^3), (3^6) であり, (1) または (2) は解 $X\in\mathcal{O}_k-\{0\}$, $u,v\in\mathcal{O}_k^\times$ を持つ. (4), (5), (6) に注意すればより詳しく, $(t)=(1)$ の時

$$X^3=1+27v,\quad v=\frac{1}{t}\in\mathcal{O}_k^\times, \tag{11}$$

$(t)=(3^6)$ の時

$$X^3=u+27,\quad u=\frac{3^6}{t}\in\mathcal{O}_k^\times, \tag{12}$$

$(t)=(3^3)$ の時

$$X^3=1+v,\quad v=\frac{3^3}{t}\in\mathcal{O}_k^\times \tag{13}$$

であることが分かる. 定理 3.3 (または定理 3.4) より (12) は不可能で, 定理 4.1 より (13) は不可能である. 定理 3.1 (または定理 3.3) より (11) が成り立つのは $k=\mathbb{Q}(\sqrt{33})$ の時のみで, $v=-\varepsilon_{33},-\varepsilon_{33}^{-1}$ である. $J(-\varepsilon_{33})=J(-\varepsilon_{33}^{-1})=-32768$ で, これらを j 不変量とする EGR を持つ楕円曲線は 2 本ある. 実際 E_2,E_2' がそう. (E_2,E_2' が $\mathbb{Q}(\sqrt{33})$ 上同型でないことは容易に確かめられる.) 故に補題 5.1 より主張が従う. □

問. 判別式が 3 乗数でない場合はどうか？定理にあるような実二次体でない場合ではどうか？

定理 5.3 ([7])**.** 実二次体 k 上 EGR を持つ global minimal な Weierstrass 方程式で定義される楕円曲線 E で, 判別式 $\Delta(E)$ が $\pm\square_k$ であり, $j(E)=J(t)$, $t\in\mathcal{O}_k$, $(t)=(1),(3^6)$ なるものが存在するのは $k=\mathbb{Q}(\sqrt{29})$ の時のみで, E は

$$\begin{aligned}
&E_3: y^2+xy+\varepsilon_{29}^2y=x^3,\\
&\qquad \Delta(E_3)=-\varepsilon_{29}^{10},\quad j(E_3)=(\varepsilon_{29}^2-3)^3/\varepsilon_{29}^4,\\
&E_4: y^2+xy+\varepsilon_{29}^2y=x^3-5\varepsilon_{29}^2x-(\varepsilon_{29}^2+7\varepsilon_{29}^4),\\
&\qquad \Delta(E_4)=-\varepsilon_{29}^{14},\quad j(E_4)=-(1+216\varepsilon_{29}^2)^3/\varepsilon_{29}^{14},
\end{aligned}$$

もしくはこれらの共役 E_3', E_4' のどれかと $\mathbb{Q}(\sqrt{29})$ 上同型である. ここで $\varepsilon_{29}=(5+\sqrt{29})/2$ は $\mathbb{Q}(\sqrt{29})$ の基本単数.

証明. 主張にあるような楕円曲線 E が存在するとせよ. $\Delta(E)\in\mathcal{O}_k^\times$ とする. (4), (5) と $\Delta(E)=\pm\square_k$ より $X^3=u+27v$, $uv=\pm\square_k$ なる $X\in\mathcal{O}_k$, $u,v\in\mathcal{O}_k^\times$ が存在する. よって定理 3.2 より $k=\mathbb{Q}(\sqrt{29})$ で, $u/v=-\varepsilon_{29}^2,-\varepsilon_{29}'^2$ である. $(t)=(1)$ ならば $t=u/v=-\varepsilon_{29}^2$, $-\varepsilon_{29}'^2$ で, $j(E)=J(-\varepsilon_{29}^2)=(\varepsilon_{29}^2-3)^3/\varepsilon_{29}^4$ または $j(E)=J(-\varepsilon_{29}'^2)=(\varepsilon_{29}'^2-2)^3\varepsilon_{29}^4$. $(t)=(729)$ ならば $t=729v/u=-729\varepsilon^2$, $-729\varepsilon'^2$ で, $j(E)=J(-729\varepsilon^2)=-(1+216\varepsilon'^2)^3\varepsilon^{14}$ または $j(E)=J(-729\varepsilon'^2)=-(1+216\varepsilon^2)^3\varepsilon'^{14}$. これらを j 不変量とする楕円曲線として E_3,E_3',E_4,E_4' が見付かっている. 故に補題 5.1 より主張が従う. □

この定理を使って, $\mathbb{Q}(\sqrt{29})$ 上 EGR を持つ楕円曲線を決定した. ([7] を参照せよ. [5] では違う証明を与えている.)

$k=\mathbb{Q}(\sqrt{733})$ の場合も (1) に解があった (定理 3.5). それと対応して $\mathbb{Q}(\sqrt{733})$ 上に EGR を持つ曲線がある ([3], [12], [24] で見付けた). 実際 $\varepsilon_{733}=(27+\sqrt{733})/2$ を $\mathbb{Q}(\sqrt{733})$ の基本単数とすると,

$$y^2+xy-\varepsilon_{733}x=x^3$$

の判別式は $-\varepsilon_{733}^5$ で, j 不変量は $J(-\varepsilon_{733})=(20457-757\sqrt{733})/2$ である. (対応する (1) の解は $(X,u,v)=(-\varepsilon_{733},-\varepsilon_{733}^5,\varepsilon_{733}^4)$ である.)

非存在に関する結果も得られている:

定理 5.4. p を $p\equiv 3 \pmod 8$, $p\neq 3,11$ なる素数とし, $k:=\mathbb{Q}(\sqrt{3p})$ とおく. ε (>1) を k の基本単数とし, $\mathfrak{P}_\infty^{(1)}$, $\mathfrak{P}_\infty^{(2)}$ を $k(\sqrt[3]{\varepsilon})$ の実無限素点とする. この時 $3\nmid h_k$ かつ

$$4\nmid h_{k(\sqrt[3]{\varepsilon})}((3)\mathfrak{P}_\infty^{(1)}\mathfrak{P}_\infty^{(2)}) \text{ または } 4\nmid h_{k(\sqrt[3]{\varepsilon},\sqrt{-3})}((\sqrt{-3}))$$

が成り立てば, k 上 EGR を持つ楕円曲線は存在しない.

証明. k 上 EGR を持つ楕円曲線が存在したとする. 定理 5.2 より E の判別式は 3 乗数ではない. h_k は奇数なので, 定理 2.6 の仮定が満たされている. よって $X^3=u+27v$ または $X^3=u+v$ を満たす $X\in\mathcal{O}_k-\{0\}$, $u,v\in\mathcal{O}_k^\times$ があるが, これは定理 3.3, 系 4.4 より不可能. □

実際に ray class number を計算して, $\mathbb{Q}(\sqrt{3p})$ $(p=43,59,67,83)$ 上 EGR を持つ楕円曲線は存在しないことが示せている. ([9] 参照.)

6 3 が分解している場合

実二次体 k で (3) が $(3)=(\pi)(\pi')$ と二つの異なる単項イデアルの積に分解している場合は,

$$X^3=\pi^3u+\pi'^3v,\quad X\in\mathcal{O}_k-\{0\},\quad u,v\in\mathcal{O}_k^\times \tag{14}$$

も考える必要がある. この時も次のことを定理 4.1 と同様に示せる. (定理 3.1 の証明法だとうまくいかないと思う.)

定理 6.1. (14) は u が 3 乗数である解を持たない.

楕円曲線はどうかというと, [23] に $\mathbb{Q}(\sqrt{997})$ 上 EGR を持ち j 不変量が $J(t)$, $(t)=(\pi^6)$ $(\pi=(221+7\sqrt{997})/2$ は 3 を割る素元で, $(\pi)\neq(\pi'))$ である楕円曲線として

$$y^2+y=x^3+x^2-(129490+4101\sqrt{997})x-\frac{50814489+1609311\sqrt{997}}{2}$$

が出ている. これの判別式は ε_{997}^2 ($\varepsilon_{997}=84906+2689\sqrt{997}$ は $\mathbb{Q}(\sqrt{997})$ の基本単数) で, j 不変量は $J(\pi^6\varepsilon_{997}^{-2})=33308803072+1054900224\sqrt{997}$ である. (対応する (14) の解は $(X,u,v)=(4\varepsilon_{997},\varepsilon_{997}^2,-\varepsilon_{997}^4)$ である.)

3 が分解する場合を研究するのも面白いとは思うが, 書いた通り π, π' がどうなるか分からないので, 難しいだろうなという気はする.

7　$S \neq \emptyset$ の場合

素イデアルの有限集合 S の外 good reduction を持つ楕円曲線を決定したいのが元々の問題であった. $S \neq \emptyset$ の時の $\mathbb{Q}$ 上での結果は数え切れないほどある. 虚二次体上では Laska, Pinch 等による多数の結果がある.

では実二次体上ではどうかというと, 筆者の知る限り, 以下の二つの結果のみである.

- ([17]) $\mathbb{Q}(\sqrt{5})$ 上で $S = \{(2)\}$ の場合. 同型類は 368 個で, 導手は $(2)^a$, $3 \leq a \leq 8$. 特に全ての曲線は (2) で additive reduction を持つ.
- ([8]) $\mathbb{Q}(\sqrt{2})$ 上で $S = \{(\sqrt{2})\}$ の場合. 同型類は 400 個で, 導手は $(\sqrt{2})^a$, $5 \leq a \leq 14$. 特に全ての曲線は $(\sqrt{2})$ で additive reduction を持つ.

どちらも面白い不定方程式が沢山出てくる. 例えば [8] では

$$\left(\frac{X(X-1)}{2}\right)^2 = \frac{Y(Y-1)}{2}$$

を満たす $X, Y \in \mathbb{Z}$ 決定することが必要になった (これは Ljunggren が既に解いていたが). [8] は職場から補助金をもらっていて, 何かする必要があり, [17] を参考にして書いたのである. こういったことをやってみたいなら, $\mathbb{Q}(\sqrt{6})$ 上で $S = \{(2+\sqrt{6})\}$ ($2+\sqrt{6}$ は 2 を割る素元) の外 good reduction を持つ楕円曲線を決定するのが面白いかもしれない. $\mathbb{Q}(\sqrt{6})$ 上 EGR を持つ楕円曲線があるので. 導手が (1) の曲線は勿論, $(2+\sqrt{6})$ の曲線 (即ち multiplicative reduction を持つ場合) なども出てくるでしょう. 同型類は 400 個どころかもっと多いかもしれない.

8　色々やることはあります

一読した方はお分かりの通り, 高校生のやるような平方完成とか, 二次方程式を解くこととか, 対称式を基本対称式で表すとか, 多少高級なことでもノルムをとって楕円曲線の整数点問題に帰着, とかそんなことしかやってない. 平田典子先生から「(1), (2) は指数型不定方程式と見た方がよい」とのご示唆をいただいたが, $\mathbb{Z}$ 上の場合と違って色々うまくいかなそうなことがあるので, あまりその方向で真剣に考えたことは無い. Baker 理論などを用いると解の個数が押さえられたりと, うまくいくことがあるかもしれない. 考えてみてください.

謝辞

コロナ禍以降色々なことがオンラインで行われるようになったこともあり, 出張するのが面倒になっていました. しかも 8 月は暑いし, ということで全然出張していませんでした. お声を掛けてくださった岸康弘氏 (愛知教育大学) には感謝してもし尽くせません. 京都駅より西に行ったのは本当に久し振りですし, 過去の研究を思い出したり, 新しいことを考えたりと, 本当に有意義な時間でした. ありがとうございました. 九州大学の金子昌信氏, 権寧魯氏, 松坂俊輝氏にも深く感謝いたします.

参考文献

[1] J. E. Cremona, Algorithms for Modular Elliptic Curves, available at `https://johncremona.github.io/book/fulltext/index.html`.

[2] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, second edition, Grad. Texts in Math., 84, Springer-Verlag, New York, 1990.

[3] H. Ishii, The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields, Japan. J. Math. (N.S.) **12** (1986), no. 1, 45–52.

[4] T. Kagawa, Determination of elliptic curves with everywhere good reduction over $\mathbb{Q}(\sqrt{37})$, Acta Arith. **83** (1998), no. 3, 253–269.

[5] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields, Arch. Math. (Basel) **73** (1999), no. 1, 25–32.

[6] T. Kagawa, Nonexistence of elliptic curves having everywhere good reduction and cubic discriminant, Proc. Japan Acad., Ser. A **76** (2000), 141–142.

[7] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields $\mathbb{Q}(\sqrt{3p})$, Acta Arith. **96** (2001), 231–245.

[8] T. Kagawa, Elliptic curves over $\mathbb{Q}(\sqrt{2})$ with good reduction outside $\sqrt{2}$, Mem. Inst. Sci. Engrg. Ritsumeikan Univ. **59** (2000), 63–79.

[9] T. Kagawa, The Diohphantine eqation $X^3 = u + 27v$ over real quadratic fields, Tokyo J. Math. **33** (2010), no. 1, 159–163.

[10] T. Kagawa, The Diohphantine eqation $X^3 = u + v$ over real quadratic fields, Bull. Pol. Acad. Sci. Math. **59** (2011), no. 1, 1–9.

[11] T. Kagawa, The Diophantine equation $X^3 = u + v$ over real quadratic fields, II, Tokyo J. Math. **44** (2021), no. 2, 507–513.

[12] M. Kida, Arithmetic of abelian varieties under field extensions, Ph.D. thesis, Johns Hopkins University, 1994.

[13] M. Kida, Computing elliptic curves having good reduction everywhere over quadratic fields, Tokyo J. Math. **24** (2001), no. 2, 545–558.

[14] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, Acta Arith. **54** (1989), no. 1, 75–80.

[15] T. Nakamura, On Shimura's elliptic curve over $\mathbb{Q}(\sqrt{29})$, J. Math. Soc. Japan **36** (1984), no. 4, 701–707.

[16] A. P. Ogg, Abelian curves of 2-power conductor, Proc. Cambridge Philos. Soc. **62** (1966), 143–148.

[17] R. G. E. Pinch, Elliptic curves with good reduction away from 2: III, preprint, arXiv:math/9803012.

[18] B. Setzer, Elliptic curves over complex quadratic fields, Pacific J. Math. **74** (1978), no. 1, 235–250.

[19] B. Setzer, Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invarinat, Illinois J. Math. **25** (1981), no. 2, 233–245.

[20] J. H. Silverman, The Arithmetic of Elliptic Curves, 2nd Edition, Grad. Texts in Math., 106 Springer, Dordrecht, 2009.

[21] J. H. Silverman and J. T. Tate, Rational Points on Elliptic Curves, 2nd Edition, Undergrad. Texts Math. Springer, Cham, 2015

[22] R. J. Stroeker, Reduction of elliptic curves over imaginary quadratic number fields, Pacific J. Math. **108** (1983), no. 2, 451–463.

[23] A. Umegaki, A construction of everywhere good $\mathbb{Q}$-curves with p-isogeny, Tokyo J. Math. **21** (1998), no. 1, 183–200.

[24] Y. Zhao, Elliptic curves over real quadratic fields with everywhere good reduction and a non-trivial 3-divison points, J. Number Theory **133** (2013), no. 9, 2901–2913.